(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 07154770 A

(43) Date of publication of application: 16 . 06 . 95

(51) Int. Cl H04N 7/167

(21) Application number: 05326166

(22) Date of filing: 30 . 11 . 93

(71) Applicant: NEC CORP

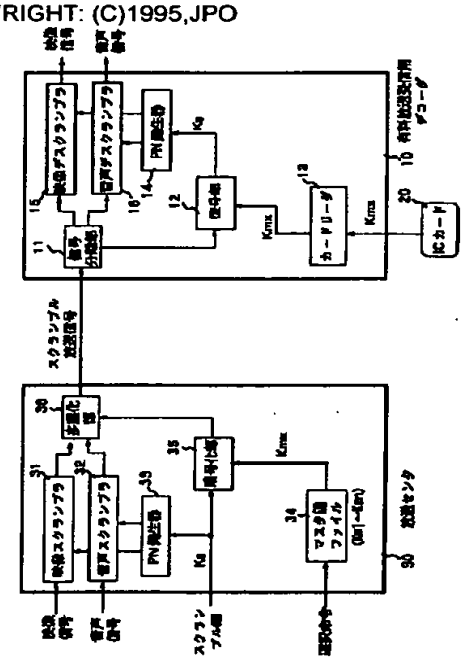
(72) Inventor: OZAKI MITSURU

(54) PAY TELEVISION BROADCAST TRANSMISSION/RECEPTION SYSTEM AND DECODER FOR RECEIVING PAY TELEVISION BROADCAST

(57) Abstract:

PURPOSE: To provide a pay television broadcast transmission/reception system and decoder capable of minimizing damage caused by illicit reception even when the state of illicit decoding the contents of a master key of one part is generated concerning the transmission/reception system for transmitting/receiving the pay television broadcast such as satellite broadcast or CATV and its decoder.

CONSTITUTION: A multiplex part 36 respectively multiplex a scramble key Ks, ciphered with a master key Kmx as a cyptographic key, to scrambled video and sound signals and transmits those signals. A decoder 10 for pay television broadcast reception reads the master key Kmx stored in an IC card 20 with a card reader 13 and decodes the scramble key Ks by inputting that master key to a decoding part 12 as a decode key. Since the master key Ks is changed periodically, it is necessary to newly purchase the IC card 20 periodically as well. The master key Kmx is used commonly for all the decoders.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－154770

(43)公開日　平成７年(1995)６月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/167				
			Ｈ０４Ｎ　7/ 167	

審査請求　有　　請求項の数４　ＦＤ　（全 10 頁）

(21)出願番号　特願平5－326166

(22)出願日　平成５年(1993)11月30日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　尾崎　満
東京都港区芝５丁目７番１号　日本電気株式会社内

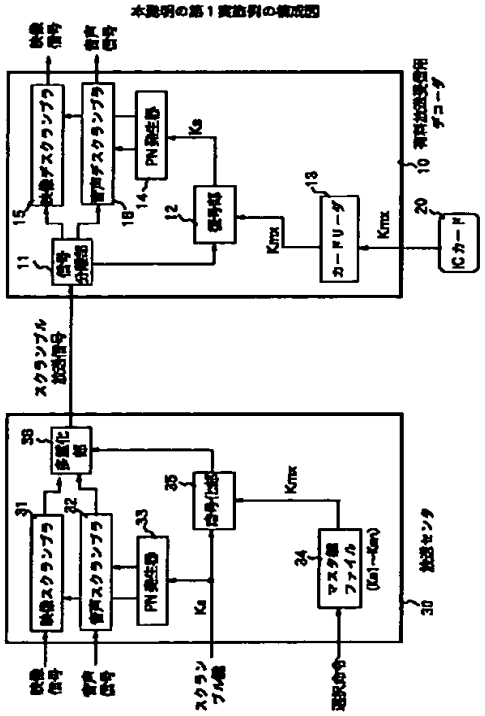
(74)代理人　弁理士　松浦　兼行

(54)【発明の名称】　有料放送送受信システム及び有料放送受信用デコーダ

(57)【要約】

【目的】　本発明は衛星放送やＣＡＴＶなどの有料放送を送受信する送受信システム及び有料放送を受信するためのデコーダに関し、一部のマスタ鍵の内容が不正に解読される事態が発生しても不正受信による被害を最小限にし得る有料放送送受信システム及び有料放送受信用デコーダを提供することを目的とする。

【構成】　多重化部３６はマスタ鍵Ｋｍｘを暗号鍵として暗号化されたスクランブル鍵Ｋｓをスクランブル処理された映像信号及び音声信号にそれぞれ多重して送信する。有料放送受信用デコーダ１０はＩＣカード２０に記憶されているマスタ鍵Ｋｍｘをカードリーダ１３で読み取り、それを復号部１２に復号鍵として入力し、スクランブル鍵Ｋｓを復号させる。マスタ鍵Ｋｓは一定期間毎に変更されるため、ＩＣカード２０も一定期間毎に新たに購入することが必要とされる。マスタ鍵Ｋｍｘは全デコーダに共通に用いられる。



1

【特許請求の範囲】

【請求項１】　擬似ランダム系列を用いて映像信号及び音声信号の少なくとも一方をスクランブル処理すると共に、該擬似ランダム系列の初期値を定めるスクランブル鍵を、マスタ鍵を暗号鍵とする暗号化処理をして前記少なくとも一方がスクランブル処理されている映像信号及び音声信号に多重し、該多重信号をスクランブル放送信号として送信し、

受信用デコーダでは、該スクランブル放送信号から前記映像信号及び音声信号と暗号化されたスクランブル鍵とをそれぞれ分離し、該暗号化されたスクランブル鍵を復号して擬似ランダム系列発生器の初期値を決定し、該擬似ランダム系列を用いて前記受信後分離した映像信号及び音声信号をデスクランブル処理する有料放送送受信システムであって、

前記送信側において前記マスタ鍵として全受信用デコーダに共通のマスタ鍵を使用すると共に該マスタ鍵を一定期間毎に変更し、

前記受信用デコーダにおいては前記暗号化されたスクランブル鍵の復号のための復号鍵として用いるマスタ鍵を、外部から挿入される記録媒体から読み取り入力することを特徴とする有料放送送受信システム。

【請求項２】　少なくとも一方がスクランブル処理されている映像信号及び音声信号と、全受信用デコーダ共通で、かつ、一定期間毎に変更されるマスタ鍵を暗号鍵として暗号化されたスクランブル鍵との多重信号であるスクランブル放送信号を受信し、少なくとも一方がスクランブル処理されている映像信号及び音声信号と、暗号化されたスクランブル鍵とをそれぞれ分離する信号分離部と、

外部より挿入される記録媒体からマスタ鍵を読み取る第１の読み取り手段と、

該第１の読み取り手段よりの該マスタ鍵を復号鍵として前記信号分離部から入力される暗号化されたスクランブル鍵を復号する復号部と、

該復号部よりのスクランブル鍵により初期値が設定される擬似ランダム系列発生器と、

該擬似ランダム系列発生器よりの擬似ランダム系列に基づいて前記信号分離部からのスクランブル処理されている映像信号及び／又は音声信号をデスクランブル処理するデスクランブラとを有することを特徴とする請求項１記載の有料放送送受信システムに用いる有料放送受信用デコーダ。

【請求項３】　前記信号分離部により分離されるスクランブル放送信号中には前記スクランブル鍵と同じマスタ鍵により暗号化された課金種別情報が含まれており、

外部より挿入される記録媒体からマスタ鍵と課金情報とを読み取り該マスタ鍵は前記復号部へ復号鍵として出力する第２の読み取り手段と、

該第２の読み取り手段により読み取られた課金情報と、

2

前記信号分離部より入力される前記課金種別情報とが入力され、該課金情報に基づいて前記擬似ランダム系列発生器へ動作許可の有無を示す信号を出力すると共に、該課金種別情報に基づいて所定の課金種別のときに新しい残度数を算出する課金制御部と、

該課金制御部により算出された新しい残度数を前記記録媒体に更新記録する記録手段とを、前記第１の読み取り手段に代えて設けたことを特徴とする請求項２記載の有料放送受信用デコーダ。

【請求項４】　前記記録媒体はＩＣカードであり、前記擬似ランダム系列発生器はＰＮ系列を発生することを特徴とする請求項２又は３記載の有料放送受信用デコーダ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は有料放送送受信システム及び有料放送受信用デコーダに係り、特に衛星放送やケーブルテレビジョン（ＣＡＴＶ）などの有料放送を送受信する送受信システム及び有料放送を受信するためのデコーダに関する。

【０００２】衛星放送やＣＡＴＶなどの有料放送では、不正受信防止のため、放送センタにおいて映像信号及び／又は音声信号（以下、「放送信号」という）を、電気的に撹拌するスクランブル処理をしてから送信することが一般的に行われる。この放送信号を受信し、正常に再生するためには、放送センタでスクランブラを動作させるのに使用したスクランブル鍵を手に入れ、このスクランブル鍵を用いて有料放送受信用デコーダ内のデスクランブラを動作させればよい。

【０００３】スクランブル鍵は通常、データ信号と混合された後、放送信号に多重化されて各受信者宅に設置されたデコーダまで配布される。従って、有料放送放送企業と正規に契約していない者が何らかの手段によりスクランブル鍵を手に入れた場合には、契約者以外の者でも容易に有料放送を不正に受信できてしまう。このため、スクランブル鍵が不正に解読されたとしても、不正受信を最小限に止める有料放送受信用デコーダが必要とされる。

【０００４】

【従来の技術】図３は文献（平成２年度の電気通信技術審議会答申諮問第４４号７６頁）に開示されている、従来の有料放送送受信システムの一例の構成図を示す。同図において、３０は放送センタ、４０は従来の有料放送受信用デコーダを示す。放送センタ３０は、映像スクランブラ３１、音声スクランブラ３２、ＰＮ発生器３３、多重化部３６、受信者別マスタ鍵ファイル３７、暗号化部３８及び３９よりなる。また、有料放送受信用デコーダ４０は、信号分離部１１、ＰＮ発生器１４、映像デスクランブラ１５、音声デスクランブラ１６、マスタ鍵記憶部４１、復号部４２、４３、及び契約条件比較回路４

４よりなる。

【０００５】放送センタ３０においては、ＰＮ発生器３３の初期値がスクランブル鍵Ｋｓにより設定され、このＰＮ発生器３３より出力されるＰＮ系列（擬似ランダム系列）を映像スクランブラ３１及び音声スクランブラ３２にそれぞれ入力して、放送する映像信号と音声信号に別々にスクランブル処理を行う。上記のスクランブル鍵Ｋｓは第三者に知られないようにするために、放送局識別情報やサービスなどの共通情報と共に暗号化部３９により暗号化される。

【０００６】ここで、スクランブル鍵Ｋｓの伝送時の暗号鍵としてワーク鍵Ｋｗが暗号化部３９に入力される。また、契約内容やデコーダＩＤなどの個別情報は受信者別マスタ鍵ファイル３７に入力されて、受信者毎（デコーダ毎）に異なるマスタ鍵Ｋｍｉが読み出される。このマスタ鍵Ｋｍｉは暗号化部３８に暗号鍵として入力され、前記ワーク鍵Ｋｗ及び個別情報の暗号化部３８での暗号に用いられる。

【０００７】映像スクランブラ３１、音声スクランブラ３２、暗号化部３８及び３９の各出力信号は多重化部３６に入力されて多重された後、スクランブル放送信号として各受信者に送信される。スクランブル鍵Ｋｓは送信、受信のＰＮ発生器３３、１４の同期のために送信される。

【０００８】有料放送受信用デコーダ４０は上記のスクランブル放送信号を受信し、多重化部３６においてそれぞれ多重された各信号を信号分離部１１にて分離する。これにより、スクランブルされた映像信号は映像デスクランブラ１５に入力され、スクランブルされた音声信号は音声デスクランブラ１６に入力され、暗号化部３８の出力暗号信号は復号部４２に入力され、更に暗号化部３９の出力暗号信号は復号部４３に入力される。

【０００９】デコーダ４０は固有のマスタ鍵Ｋｍｉを記憶している記憶部４１を有しており、このマスタ鍵Ｋｍｉを用いて復号部４２により復号動作を行わせ、受信したスクランブル放送信号中のワーク鍵Ｋｍ及び個別情報を復号する。復号されたワーク鍵Ｋｗは復号部４３に復号鍵として入力され、ここで受信したスクランブル放送信号中のスクランブル鍵Ｋｓ及び共通情報をそれぞれ復号させる。

【００１０】復号部４２より取り出された個別情報及び復号部４３より取り出された共通情報は、それぞれ契約条件比較回路４４に入力され、ここで所定の契約条件を満足するか否か自動的に判定される。契約条件を満足するときには契約条件比較回路４４からＰＮ発生器１４へ作動信号が出力される。このＰＮ発生器１４は作動信号が入力され、かつ、復号部４３より正しいスクランブル鍵Ｋｓが入力されたときに、放送センタ３０内のＰＮ発生器３３より出力されるＰＮ系列と同じＰＮ系列を発生し、映像デスクランブラ１５及び音声デスクランブラ１６にそれぞれ入力する。

【００１１】このようにして、映像デスクランブラ１５からはスクランブル処理が解除された映像信号が取り出され、また音声デスクランブラ１６からはスクランブル処理が解除された音声信号が取り出される。

【００１２】なお、従来の有料放送受信用デコーダには、契約条件比較回路４４での契約条件比較を外部からのカードから読み取った課金条件なども含めて比較するものも知られている（例えば、特開平２－１１１１８５号公報）。

【００１３】

【発明が解決しようとする課題】従来の有料放送受信用デコーダ４０においては、デコーダ毎に設定された復号用マスタ鍵Ｋｍｉ（ここでｉはデコーダ毎に付与されたＩＤ番号）は、ＩＣチップの形態でデコーダ４０内に４１で示す如く組み込まれており、容易に取り外しができない構造とされている。

【００１４】しかしながら、図３に示した従来の有料放送受信用デコーダや、カードにより課金条件を入力するような従来の有料放送用デコーダでは、マスタ鍵Ｋｍｉはデコーダ内にハードウェアの形態で内蔵されているため、ひとたびマスタ鍵Ｋｍｉの内容が不正に解読された場合には、ワーク鍵Ｋｗ及びスクランブル鍵Ｋｓがそれぞれ復号されてしまい、これに対抗する手段がない。唯一、放送センタ側のマスタ鍵ファイル３７中の該当するマスタ鍵Ｋｍｉを変更すれば対抗することができるが、どのマスタ鍵が解読されたかを知る方法がないことから事実上該当するマスタ鍵Ｋｍｉだけを変更することは不可能である。また、マスタ鍵ファイル３７の内容を全面的に変更するのでは、正規にデコーダを購入して所有している受信者が受信できなくなってしまう。

【００１５】また、放送センタ３０側では、各デコーダで異なるマスタ鍵情報のうち料金滞納者や契約終了者などの分を除いた正規加入者分のすべてのマスタ鍵を送出しなければならず、このため加入者数が増えれば増えるほど煩雑で時間のかかる作業を行う必要がある。

【００１６】本発明は以上の点に鑑みなされたもので、一定期間毎にマスタ鍵の内容を変更することにより、一部のマスタ鍵の内容が不正に解読される事態が発生しても不正受信による被害を最小限にし得る有料放送送受信システム及び有料放送受信用デコーダを提供することを目的とする。

【００１７】

【課題を解決するための手段】上記の目的を達成するため、本発明の有料放送送受信システムは擬似ランダム系列を用いて映像信号及び音声信号の少なくとも一方をスクランブル処理すると共に、擬似ランダム系列の初期値を定めるスクランブル鍵を、マスタ鍵を暗号鍵とする暗号化処理をして前記映像信号及び音声信号に多重してスクランブル放送信号として送信し、受信用デコーダで

は、スクランブル放送信号から前記映像信号及び音声信号と暗号化されたスクランブル鍵とをそれぞれ分離し、暗号化されたスクランブル鍵を復号して擬似ランダム系列発生器の初期値を決定し、擬似ランダム系列を用いて前記受信後分離した映像信号及び音声信号をデスクランブル処理する有料放送送受信システムであって、送信側において前記マスタ鍵として全受信用デコーダに共通のマスタ鍵を使用すると共にマスタ鍵を一定期間毎に変更し、受信用デコーダにおいては前記暗号化されたスクランブル鍵の復号のための復号鍵として用いるマスタ鍵を、外部から挿入される記録媒体から読み取り入力する構成としたものである。

【００１８】また、本発明の有料放送受信用デコーダでは、前記スクランブル放送信号を受信し、少なくとも一方がスクランブル処理されている映像信号及び音声信号と、暗号化されたスクランブル鍵とをそれぞれ分離する信号分離部と、外部より挿入される記録媒体からマスタ鍵を読み取る第１の読み取り手段と、第１の読み取り手段よりのマスタ鍵を復号鍵として信号分離部から入力される暗号化されたスクランブル鍵を復号する復号部と、復号部よりのスクランブル鍵により初期値が設定される擬似ランダム系列発生器と、擬似ランダム系列に基づいて信号分離部からのスクランブル処理されている映像信号及び／又は音声信号をデスクランブル処理するデスクランブラとを有する構成としたものである。

【００１９】更に、請求項３記載の有料放送受信用デコーダでは、外部より挿入される記録媒体からマスタ鍵と課金情報とを読み取りマスタ鍵は復号部へ復号鍵として出力する第２の読み取り手段と、この課金情報と信号分離部より入力される課金種別情報とが入力され、課金情報に基づいて擬似ランダム系列発生器へ動作許可の有無を示す信号を出力すると共に、課金種別情報に基づいて所定の課金種別のときに新しい残度数を算出する課金制御部と、この新しい残度数を記録媒体に更新記録する記録手段とを、前記請求項２記載の有料放送受信用デコーダの第１の読み取り手段に代えて設けた構成としたものである。

【００２０】

【作用】本発明の有料放送送受信システムでは、送信スクランブル放送信号中のマスタ鍵を一定期間毎に変更するようにしているため、外部からデコーダに挿入される記録媒体も送信スクランブル放送信号中のマスタ鍵に対応して一定期間毎に同じマスタ鍵が記録された記録媒体に変更するようにさせることができる。

【００２１】また、請求項２記載の有料放送受信用デコーダでは、第１の読み取り手段により、外部から挿入される記録媒体から読み取るマスタ鍵は、受信者対応のものではなく、すべての受信者（すべてのデコーダ）に共通の同一のマスタ鍵であるため、有料放送受信用デコーダをすべての受信者に共通の構成とすることができる。また、外部から記録媒体を挿入するだけで有料放送を受信することができる。

【００２２】更に、請求項３記載の有料放送受信用デコーダでは、課金種別が所定の種別のときには、課金制御部により新しい残度数を算出し、その残度数を記録手段により記録媒体に更新記録するようにしているため、送信側では残度数を管理する必要がなく、記録媒体に記録されている常に最新の残度数に基づく有料放送受信ができる。

【００２３】

【実施例】次に、本発明の実施例について説明する。図１は本発明の第１実施例の構成図を示す。同図中、図３と同一構成部分には同一符号を付してある。図１において、１０は本発明の有料放送受信用デコーダの第１実施例で、信号分離部１１、復号部１２、カードリーダ１３、ＰＮ発生器１４、映像デスクランブラ１５及び音声デスクランブラ１６より構成されている。

【００２４】カードリーダ１３はＩＣカード２０の記録情報を読み取る機器で、前記第１の読み取り手段を構成している。また、ＩＣカード２０は受信しようとするスクランブル放送信号中の暗号化されているスクランブル鍵Ｋｓを復号するための復号鍵となるマスタ鍵Ｋｍｘが記録されている記録媒体である。ＰＮ発生器１４は擬似ランダム系列であるＰＮ系列を発生する回路で、その初期値はスクランブル鍵Ｋｓにより設定される。

【００２５】３０は放送センタで、有料放送受信用デコーダ１０と共に有料放送送受信システムを構成している。放送センタ３０は映像スクランブラ３１、音声スクランブラ３２、ＰＮ発生器３３、マスタ鍵ファイル３４、暗号化部３５及び多重化部３６より構成されている。ＰＮ発生器３３はＰＮ発生器１４と同一構成の擬似ランダム系列発生器である。また、マスタ鍵ファイル３４は多数のマスタ鍵Ｋｍ１～Ｋｍｎを収納しており、外部からの選択命令によりそのうちのひとつのマスタ鍵Ｋｍｘが選択される。このマスタ鍵Ｋｍｘは一定期間毎（例えば６ケ月毎）に変更されるようになされている。

【００２６】ところで、有料放送の契約内容としては、チャンネル毎に月極めで定額料金を支払うことによりそのチャンネルのすべての番組を視聴することができるフラットフィー、いくつかの番組及び料金設定方式を組み合わせた番組表や料金一覧表を用意し、この中から視聴者が選択して契約するティア、個別番組毎に料金を設定し、視聴した番組だけに課金するペイパープログラム、単位時間毎に所定の料金が設定されており、視聴した時間分に課金するペイパータイムなどがある。本実施例は、このうち、フラットフィー方式の有料放送に有効なシステムである。

【００２７】次に、本実施例の動作について説明する。まず、放送しようとする映像信号及び音声信号はそれぞれ対応する映像スクランブラ３１及び音声スクランブラ

３２に入力され、ここでＰＮ発生器３３より供給されるＰＮ系列に基づきスクランブル処理が行われる。スクランブル処理の具体的方法は種々提案されている（例えば映像信号に関しては走査線内信号切替方式、走査線転移方式、あるいはこれらの併用方式など、また音声信号に関してはＰＮ信号系列加算方式など）が、これらは公知であり、また本発明の要旨ではないのでその詳細な説明は省略する。

【００２８】上記の映像スクランブラ３１及び音声スクランブラ３２におけるスクランブラに用いられるＰＮ系列の初期値は、スクランブル鍵Ｋｓにより設定される。このスクランブル鍵Ｋｓは暗号化部３５に入力され、ここでマスタ鍵ファイル３４から選択命令に従って読み出されたマスタ鍵Ｋｍｘを暗号鍵として暗号化される。マスタ鍵Ｋｍｘはすべての受信用デコーダに共通に用いられ、また、前記したように一定期間毎に変更される。

【００２９】暗号化されたスクランブル鍵Ｋｍｘと映像スクランブラ３１及び音声スクランブラ３２よりそれぞれスクランブル処理されて取り出された映像信号及び音声信号とは多重化部３６において多重化される。この多重化部３６より取り出された多重信号はスクランブル放送信号として無線又は有線にて送信される。

【００３０】有料放送受信希望者（加入者）は、有料放送放送局（又はその代行者）から有料放送受信用デコーダ１０とＩＣカード２０とを料金前払いで購入する。ＩＣカード２０にはマスタ鍵情報（ここではＫｍｘ）が予め記録されている。このＩＣカード２０は有料放送受信用デコーダ１０内に挿入されることにより、カードリーダ１３でその記録情報が読み取られ、そのうちマスタ鍵Ｋｍｘが復号部１２に復号鍵として入力される。

【００３１】一方、有料受信用デコーダ１０はスクランブル放送信号を受信し、信号分離部１１により受信信号からスクランブル処理されている映像信号と、スクランブル処理されている音声信号とをそれぞれ分離して映像デスクランブラ１５及び音声デスクランブラ１６にそれぞれ入力すると共に、受信信号から暗号化されているスクランブル鍵Ｋｓを分離して復号部１２に入力する。

【００３２】復号部１２はこの暗号化されているスクランブル鍵Ｋｓを、カードリーダ１３からのマスタ鍵Ｋｍｘを復号鍵として復号し、放送センタ３０において用いられたスクランブル鍵Ｋｓを復号する。復号されたスクランブル鍵ＫｓはＰＮ発生器１４に入力されてその出力ＰＮ系列の初期値を定める。

【００３３】これにより、ＰＮ発生器１４からは放送センタ３３より出力されたＰＮ系列と同期したＰＮ系列が取り出され、映像デスクランブラ１５及び音声デスクランブラ１６にそれぞれ供給されてデスクランブラ処理を行わせる。その結果、映像デスクランブラ１５及び音声デスクランブラ１６からは、それぞれスクランブルが解除された正常な映像信号及び音声信号が取り出される。

【００３４】本実施例では、マスタ鍵Ｋｍｘは一定期間後に別の値のマスタ鍵（例えばＫｍｙ）に変更される。このため、マスタ鍵Ｋｍｘの情報が記録されているＩＣカード２０を用いても有料放送を受信することができなくなる。そこで、受信希望者は新しいマスタ鍵Ｋｍｙの情報が記録されている別のＩＣカードを新たに購入して、これを有料放送受信用デコーダ１０に挿入することにより、再び受信することができる。

【００３５】従って、何らかの手段によりスクランブル鍵Ｋｓあるいはマスタ鍵Ｋｍｘが不正に解読されたときには、従来では何らの対抗手段もなかったが、本実施例によれば、最長でも上記の一定期間のみしか不正視聴ができないため、不正視聴による被害を最小限に止めることができる。

【００３６】また、本実施例ではマスタ鍵Ｋｍｘなどはすべての有料放送受信用デコーダ１０に共通であるため、有料放送受信用デコーダ１０はすべて同一構成とすることができるため、デコーダ製造コストを従来よりも安価にすることができ、更に従来の放送センタでの受信者対応のマスタ鍵ファイル作成作業の煩雑さを除去することができる。また、本実施例では、有料放送受信用デコーダ１０を動作させるためにはＩＣカード２０を料金前払いで購入する必要があるため、従来生じていた長期滞納者に対する送信停止前の既放送分の料金の未回収を防止することができる。

【００３７】次に、本発明の第２実施例について説明する。図２は本発明の第２実施例の構成図を示す。同図中、図１と同一構成部分には同一符号を付し、その説明を省略する。図２において、１０´は本発明の有料放送受信用デコーダの第２実施例で、第１実施例のカードリーダ１３に代えて、カードリーダ／ライタ１８及び課金制御部１９が設けられている点に特徴がある。

【００３８】カードリーダ／ライタ１８はＩＣカードの記録情報を読み取る機能と、ＩＣカードに入力情報を書き込む機能とをそれぞれ有する機器で、前記した第２の読み取り手段及び記録手段とを構成している。また、放送センタ３０内の暗号化部３５´はスクランブル鍵Ｋｓと共に課金種別情報も併せて暗号化する構成とされている。本実施例はペイパービュー（すなわち、ペイパープログラム及びペイパータイム）に有効な有料放送送受信システムである。

【００３９】次に、本実施例の動作について説明する。放送センタ３０では、暗号化部３５´において、スクランブル鍵Ｋｓと共に放送番組がフラットフィーであるかペイパービュー（すなわち、ペイパープログラム及びペイパータイム）であるかを示す課金種別情報が、マスタ鍵ファイル３４からのマスタ鍵Ｋｍｘを暗号鍵として暗号化される。

【００４０】この暗号化部３５´で暗号化されたスクランブル鍵Ｋｓ及び課金種別情報は、多重化部３６におい

て映像スクランブラ３１及び音声スクランブラ３２よりそれぞれスクランブル処理されて取り出された映像信号及び音声信号と多重化されてスクランブル放送信号とされて無線又は有線にて送信される。

【００４１】有料放送受信希望者（加入者）は、有料放送放送局（又はその代行者）から有料放送受信用デコーダ１０´とＩＣカード２１とを料金前払いで購入する。ＩＣカード２１にはマスタ鍵情報（ここではＫｍｘ）と共に、その受信希望者の残度数を示す課金情報が予め記録されている。このＩＣカード２１は有料放送受信用デコーダ１０´内に挿入されることにより、カードリーダ／ライタ１８でその記録情報が読み取られ、そのうちマスタ鍵Ｋｍｘが復号部１２に復号鍵として入力され、課金情報が課金制御部１９へ入力される。

【００４２】一方、有料放送受信用デコーダ１０´は放送センタ３０から送信されたスクランブル放送信号を受信し、信号分離部１１により受信信号からスクランブル処理されている映像信号と、スクランブル処理されている音声信号とをそれぞれ分離して映像デスクランブラ１５及び音声デスクランブラ１６にそれぞれ入力すると共に、受信信号から暗号化されているスクランブル鍵Ｋｓと課金種別情報とを分離して復号部１２に入力する。

【００４３】課金制御部１９はカードリーダ／ライタ１８より入力されるＩＣカード２１に記録されていた課金情報に基づいて残度数を調べ、残度数がゼロでないときに限り、ＰＮ発生器１４に動作許可信号（命令）を送出する。ＰＮ発生器１４はこの動作許可信号が入力されている場合に限り、復号化部１２からのスクランブル鍵Ｋｓに基づくＰＮ系列を発生して映像デスクランブラ１５及び音声デスクランブラ１６にそれぞれ供給し、それぞれスクランブル処理が解除された映像信号及び音声信号を出力させる。

【００４４】また、課金制御部１９は復号部１２から入力される前記課金種別情報に基づき、現在受信中の番組がフラットフィーであるかペイパービューであるかを識別し、受信中は有料放送受信用デコーダ１０´内に挿入された状態で保持されているＩＣカード２１に対して、ペイパービューと識別した場合に限り、ペイパープログラムかペイパータイムかの種類に応じて規定料金を算出し、その算出した規定料金分の度数をＩＣカード２１の残度数から減じて新しい残度数を書き込む動作を繰り返す。

【００４５】本実施例も第１実施例と同様に、マスタ鍵Ｋｍｘは一定期間後に別の値のマスタ鍵（例えばＫｍｙ）に変更される。このため、マスタ鍵Ｋｍｘの情報が記録されているＩＣカード２１を用いても有料放送を受信することができなくなる。そこで、受信希望者は新しいマスタ鍵Ｋｍｙの情報と課金種別情報とが記録されている別のＩＣカードを新たに購入して、これを有料放送受信用デコーダ１０´に挿入することにより、再び受信することができる。

【００４６】従って、本実施例も何らかの手段によりスクランブル鍵Ｋｓあるいはマスタ鍵Ｋｍｘが不正に解読されたときでも、不正視聴による被害を最小限に止めることができるなどの第１実施例と同様の特長を有すると共に、それに加えてＩＣカード２１の残度数を更新記録するようにしているため、課金を確実に行えるという特長がある。

【００４７】なお、本発明は以上の実施例に限定されるものではなく、例えばマスタ鍵Ｋｍｘや課金情報を記録する記録媒体はＩＣカード以外の磁気カード、コンパクトディスク、磁気ディスクその他の記録媒体でもよく、またマスタ鍵ファイル３４の代わりに選択指令に応じて所望のマスタ鍵を自動生成する回路を用いることにより、記憶容量の制限をなくすようにしてもよい。また、本発明は映像信号及び音声信号のどちらか一方のみに対してスクランブル処理を行う有料放送送受信システムにも適用することができることは勿論である。

【００４８】

【発明の効果】以上説明したように、本発明の有料放送送受信システムによれば、デコーダを動作させるために必要な外部からデコーダに挿入される記録媒体を、スクランブル放送信号中のマスタ鍵に対応して一定期間毎に同じマスタ鍵が記録された記録媒体に変更しなければならないようにしたため、何らかの手段によりスクランブル鍵あるいはマスタ鍵が不正に解読されたときでも、従来に比べてデコーダの構造を複雑にすることなく、不正視聴による被害を最小限に止めることができ、また、従来の放送センタでの受信者対応のマスタ鍵ファイル作成作業の煩雑さを除去することができる。

【００４９】また、本発明の有料放送受信用デコーダによれば、すべての受信者（すべてのデコーダ）に共通の同一のマスタ鍵が記録された記録媒体を使用することにより、有料放送受信用デコーダをすべての受信者に共通の構成とすることができるようにしたため、デコーダ製造コストを従来よりも安価にすることができる。

【００５０】更に、本発明の有料放送受信用デコーダによれば、課金種別が所定の種別のときには、課金制御部により新しい残度数を算出し、その残度数を記録手段により記録媒体に更新記録することにより、送信側では残度数を管理する必要がなく、記録媒体に記録されている常に最新の残度数に基づく有料放送受信ができるようにしたため、課金が確実にできる。

【図面の簡単な説明】

【図１】本発明の第１実施例の構成図である。

【図２】本発明の第２実施例の構成図である。

【図３】従来の有料放送送受信システムの一例の構成図である。

【符号の説明】

１０、１０´　有料放送受信用デコーダ

11

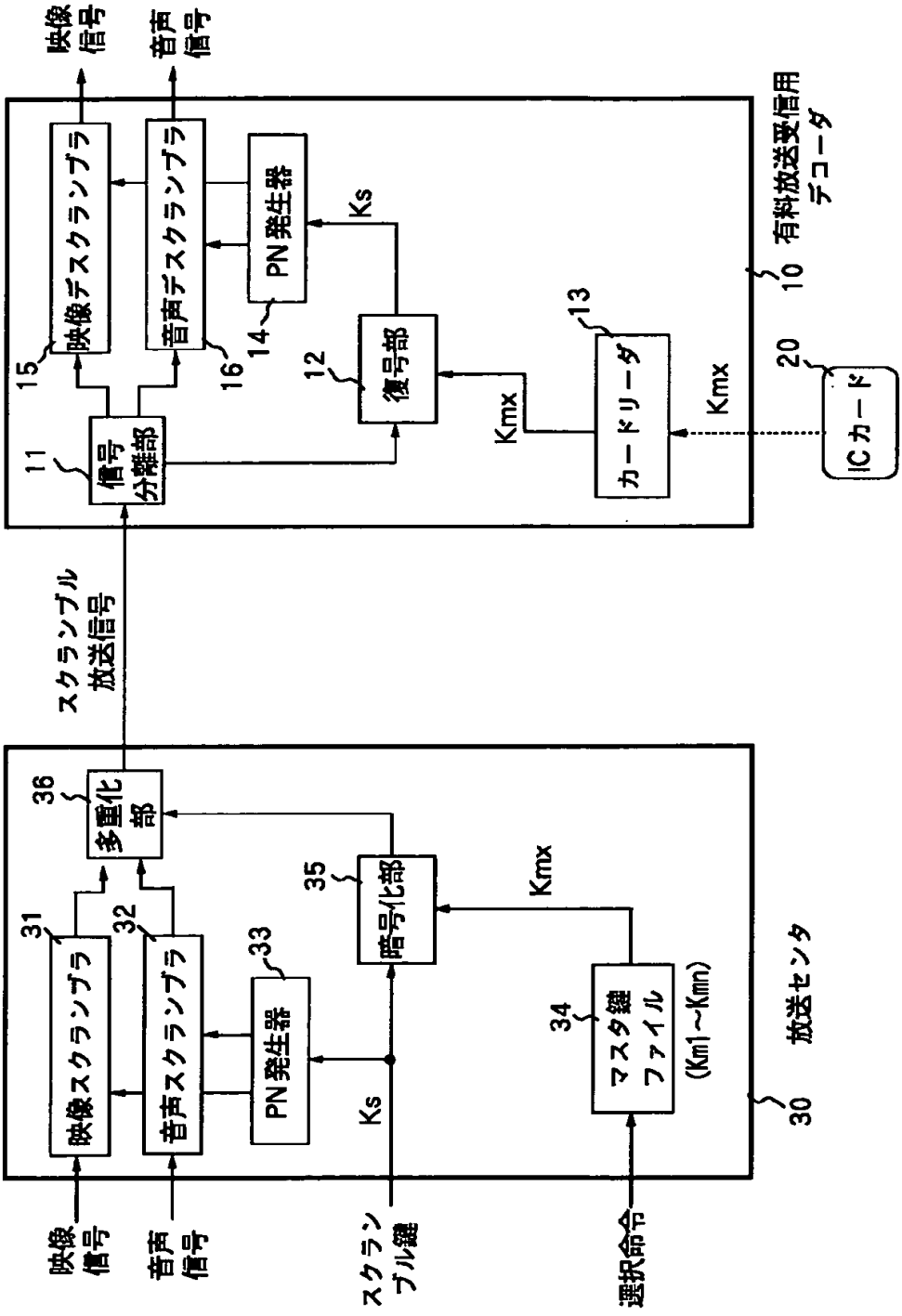
１１　信号分離部
１２　復号部
１３　カードリーダ
１４、３３　ＰＮ発生器
１５　映像デスクランブラ
１６　音声デスクランブラ

12

＊１８　カードリーダ／ライタ
１９　課金制御部
２０、２１　ＩＣカード
３０　放送センタ
３４　マスタ鍵ファイル
＊　３５、３５´　暗号化部

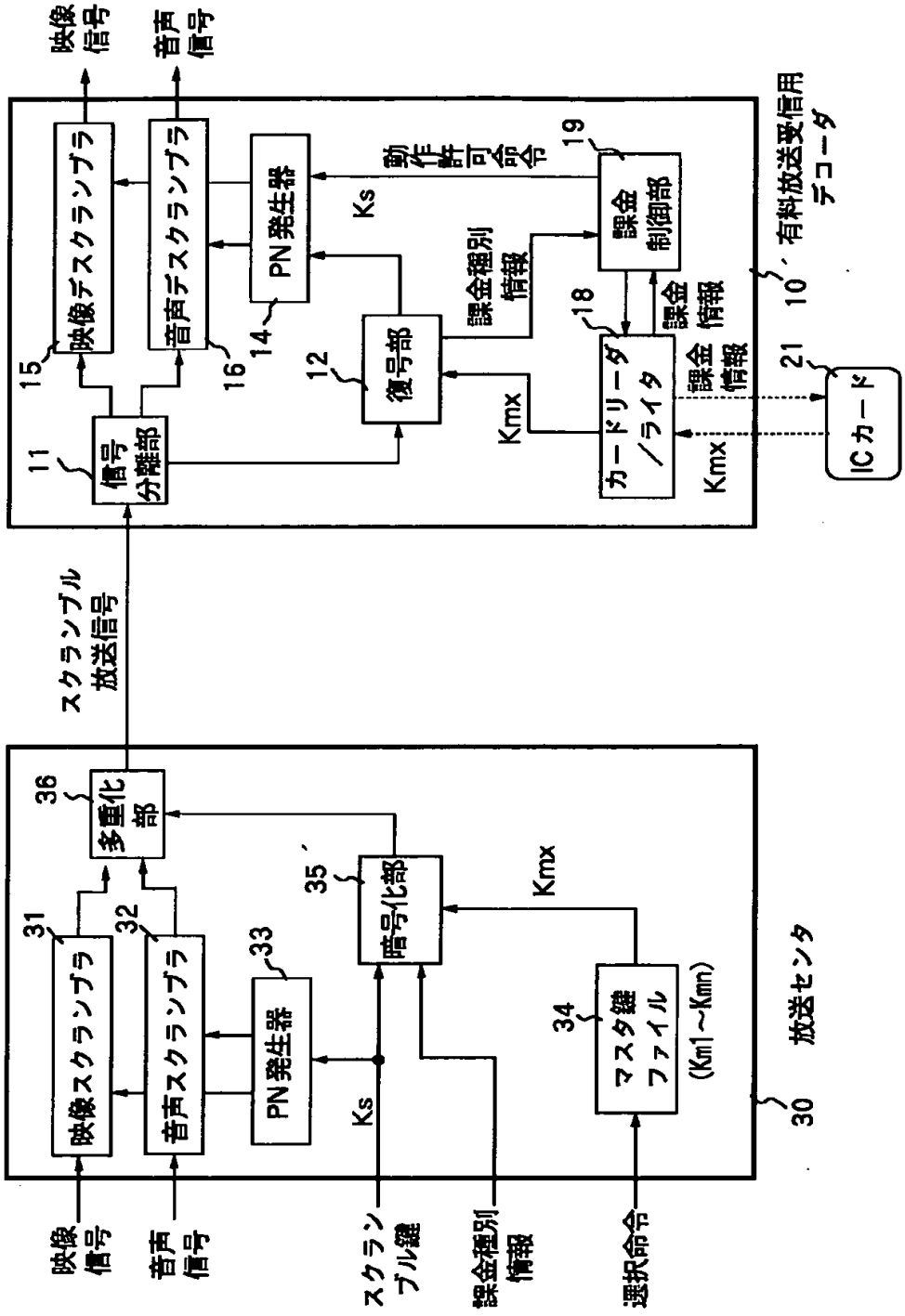
【図１】

本発明の第１実施例の構成図



【図２】

本発明の第２実施例の構成図



【図３】

従来の有料放送送受信システムの一例の構成図